PA/129 326/PCT

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

CORRECTED VERSION

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 January 2001 (11.01.2001)

PCT

(10) International Publication Number
WO 01/03077 A1

(51) International Patent Classification[7]: G07D 7/00, G07F 7/08

(21) International Application Number: PCT/IB00/00908

(22) International Filing Date: 5 July 2000 (05.07.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
99/4367 5 July 1999 (05.07.1999) ZA

(71) Applicant *(for all designated States except US)*: DEXRAD (PROPRIETARY) LIMITED [ZA/ZA]; BP House, 10 Junction Road, 2193 Parktown (ZA).

(72) Inventor; and

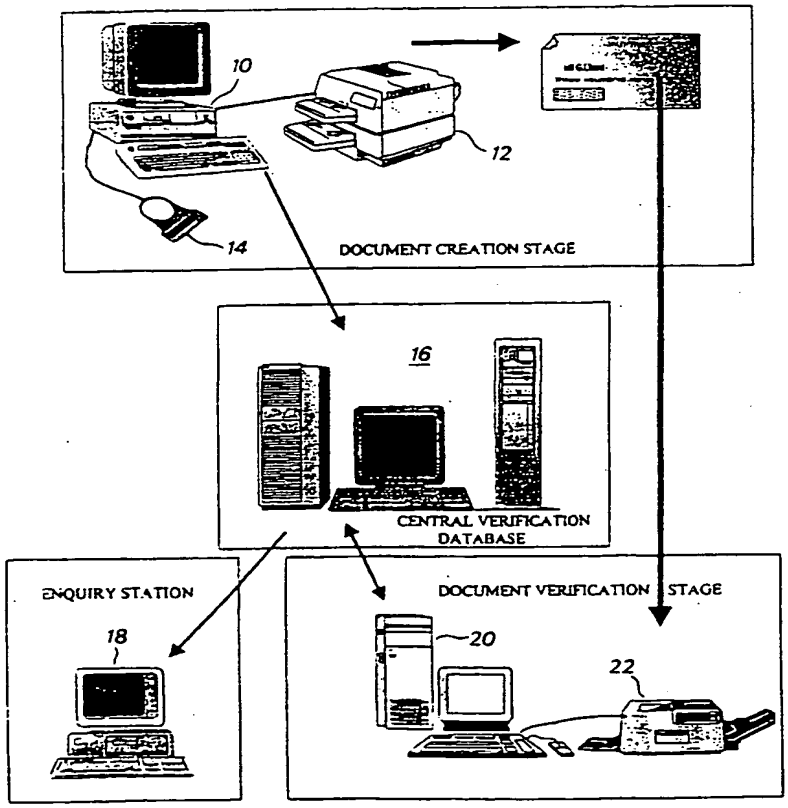
(75) Inventor/Applicant *(for US only)*: TAME, Gavin, Randall [ZA/ZA]; 346 Schoongezicht Street, Erasmusrand, 0181 Pretoria (ZA).

(74) Agents: DE VILLIERS, Christopher, Murray et al.; Spoor And Fisher, Rochester Place, 173 Rivonia Road, Morningside, Sandton, P.O. Box 41312, 2024 Craighall (ZA).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

[Continued on next page]

(54) Title: DOCUMENT VERIFICATION SYSTEM



(57) Abstract: A method of generating documents and verifying their authenticity firstly requires controler access to a document creation system so that only authorised users can create documents. User data which identifies a user of the system is recorded, and verification data is generated from both the user data and data corresponding to documents generated using the system. Authentication data corresponding to the verification data is recorded, and the document is then printed with a machine readable portion containing the verification data. The machine readable portion is typically a two dimensional bar code or symbol. When the document is presented, the verification data is read from it, for example by optical scanning, and compared with retrieved authentication data to indicate whether or not the document is authentic.

WO 01/03077 A1

(84) **Designated States** *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

(48) **Date of publication of this corrected version:**
29 March 2001

(15) **Information about Correction:**
see PCT Gazette No. 13/2001 of 29 March 2001, Section II

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

1/prts

DOCUMENT VERIFICATION SYSTEM

BACKGROUND OF THE INVENTION

THIS invention relates to a method of generating a document, a method of verifying the authenticity of a document and to a system for implementing the methods.

Document fraud, particularly relating to documents of monetary value such as cheques, is increasingly prevalent and causes huge financial losses both to financial institutions and the general public. Various attempts have been made to reduce such fraud, but existing methods such as the use of identification cards by persons wishing to cash a cheque can be onerous for the users thereof, and are in any case still subject to fraud.

It is an object of the invention to provide an alternative method and system of generating documents and verifying the authenticity of such documents.

SUMMARY OF THE INVENTION

According to the invention there is provided a method of generating a document comprising the steps of:

permitting access to a document creation system by an authorised user;

recording user data identifying the user;

generating document data defining a document;

generating verification data from the user data and the document data;

recording authentication data corresponding to the verification data; and

printing the document utilising the document data and the verification data, so that the document includes a machine readable portion usable to verify the authenticity thereof.

The method may include generating a user identification record and storing the record for comparison with the user data when a user attempts to access the document creation system.

The user data and the user identification record may comprise data from a fingerprint scanner or another biometric device, for example.

The user data may be derived from data stored on a portable data carrier such as a smart card, the user data being generated when a physical characteristic of the user, such as a fingerprint, matches data stored on the portable data carrier.

The authentication data may be stored in a document verification database.

The verification data may take the form of a bar code, symbol or other machine readable indicium.

Preferably, the verification data is a printed symbol or code readable optically, and contains data which corresponds at least partially to the user data and the related document data contained in the authentication data which is stored in the document verification database.

The verification data is preferably generated in an encrypted form.

The invention extends to a method of verifying the authenticity of a document generated by the above-defined method, including the steps of:

reading verification data from the document;

retrieving authentication data corresponding to the verification data and comparing the verification data with the authentication data; and

indicating that the document is authentic if the compared data matches.

In the case where the verification data is encrypted, the method will include the step of decrypting the verification data read from the document.

The authentication data may be retrieved from a central database in an on-line process.

Alternatively, the authentication data may be data derived from the document itself, or from a bearer thereof, for example.

The invention includes a system for generating documents comprising:

a document creation station operable by a user to input document data and to generate printed documents based on the document data;

access control means arranged to generate user data corresponding to an authorised user;

processor means for generating verification data derived from the document data and the user data, the verification data being applied to the printed document; and

a database for storing an authentication record corresponding to the verification data, for use in authentication of the document.

The system preferably includes at least one document reading device for reading the verification data on a document, and processor means for comparing the verification data read from the document with authentication data.

The system preferably further includes communication means for transferring authentication data from the database, for comparison with the verification data read from the document.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a highly schematic block diagram of a document creation and verification system according to the invention.

DESCRIPTION OF EMBODIMENTS

In general, the present invention aims to provide a method and system for generating documents the authenticity of which can readily be verified, and to a method and system for verifying such documents.

In this specification, although the invention is described primarily with reference to cheques, being documents having a monetary value, it will be appreciated that the application of the invention is not limited to cheques, and that the invention can be applied to the verification of vouchers, certificates, identification documents and many other kinds of valuable documents. The invention could also, for example, be applied to document labelling such as bills of lading and other transportation documents or labels.

The main aim of the invention is to provide relatively secure and tamper proof methods of issuing/creating, distributing and verifying the authenticity of documents. The invention also provides accountability throughout the document creation/management process, and was designed in order to prevent the fraudulent manipulation of or tampering with documents throughout their life cycle. Specifically in the case of cheques, the invention aims to prevent fraudulent manipulation and tampering from the time of creation of a cheque (ie. entering the cheque data and printing the cheque) through to the final verification of the authenticity of a presented cheque and approval for payment thereof.

The methodology of the invention can be split into three main stages:

a document creation stage,
a document distribution stage, and
a document verification stage.

The distribution of the documents is mentioned primarily for completeness. It is significant that, due to the inherent security of documents created by the method of the invention, the method of distribution of the documents can be flexible. This is because each document carries its own verification data, and the document can be verified at any stage of its distribution.

The document verification stage is an important component of the invention, by means of which documents are checked for authenticity. For example, the authenticity of a cheque may be verified before it is paid. Such verification may be carried out on-line, either manually or in an automated process, or off-line in certain applications.

Central to the above three stages is a document verification database, which holds a complete record of all documents created. The document verification database contains a duplicate of verification data which is printed on the document itself, enabling future verification thereof. In order to hinder fraud, sophisticated encryption techniques are used to generate and print the verification data.

The various aspects of the invention are described in greater detail below.

Figure 1 shows, in a simplified block diagram form, the main components which form the system of the invention. Documents are created at a document creation station using a computer 10 (typically a personal computer or PC) with an associated high quality printer 12. Documents can also be created by a

mass production printer using font based symbols (as opposed to the normal image based symbols). Such font based symbols do not slow down production capacity. A scanner 14 is connected to the computer 10 and is used to identify a user of the system.

Connected to the computer 10, typically via modems which access an existing telecommunications network, or another means of communicating over a wide area, is a central verification database 16. Apart from the computer 10 (and others like it) enquiry stations 18 and document verification stations 20 are connected to the database 16. Each document verification station will typically comprise a computer 20 with an associated high speed scanner/feeder 22.

In order to control access to the document creation station, authorised users are provided with access cards or identity cards which contain encrypted machine readable data identifying the user. The data is preferably biometric in nature, such as fingerprint data. A fingerprint scanning unit is used to acquire a fingerprint of the user, and the fingerprint biometric data, together with other data identifying the user, is compressed and encrypted and encoded into a two-dimensional code or symbol which is printed on the access card.

To use the document creation system, a user presents the card to a reader, which scans and decodes the symbol on the card and retrieves the fingerprint biometric data therefrom, as well as other data identifying the user. At the same time, the user places his/her finger in a fingerprint scanner, and the "live" scanned fingerprint is compared with the biometric data stored on the card. If these details match, the user's details read from the card are entered into a user log together with the current date and time, and access is granted to the document creation station. The user data log can be used subsequently to establish accountability.

In an alternative embodiment, instead of using an access card with an encrypted, printed symbol thereon, a smart card containing data in its embedded memory chip, encrypted to a suitable level, can be used instead. In either case, the data on the access card can include data relating to the level of the document creation system to which the user has access. In another alternative embodiment, the user can use a "live" fingerprint scan which is compared to a database of fingerprints (a one to many match).

From the abovementioned user data and other relevant data such as the date and time and the details of the document itself, verification data is generated. This data will be applied to the document which is created, and is also stored in the verification database as an authentication record, which means that a complete record of the document exists on the database. Typically, the verification data will consist of one or more of the following (although it is not restricted to these):

1. details of an operator generating the document;
2. date/time stamps;
3. unique document and/or institution code;
4. partial or relevant details from the document (example: monetary amounts);
5. digital signatures of the operator and/or competent authority;
6. digital certificates;
7. fingerprint or other biometric data;
8. textual information.

For printing on the document, the verification data is compressed and encrypted, and printed in a two dimensional graphic format or font format, as a symbol or code. The data compression and encryption processes are now described.

The encryption of the verification data is an important part of the process as the protection of the symbol against fraudulent onslaughts depends on the strength of the encryption. The encryption used can be divided into two distinct parts, namely private/public key encryption (Asymmetric Encryption) and multi-layered core encryption.

The public/private key encryption takes care of two aspects of authority. The first is the authority to create the verification data of a document. The second part is the authority to decode the verification data. The former is based on a private key, which is entered into the user's machine readable access card by an administrator of the system. This private key encrypts the data. The private key allows for the creation of a specific public key which creates the latter part, an authority to view the verification data. The public key allows for the decoding or access to the verification data within the two dimensional bar code.

The private key can only be created with the private creation system which allows a person in authority to create this key.

The multi-layered encryption system is an inner layer of encryption beneath the above mentioned private/public key layer. This encryption makes use of three distinct encryption methods, which are completely different from each other. Two of the encryption methods are data scrambling algorithms. The third layer is a form of encryption which allows for each symbol created to be uniquely encrypted. This layer creates the strongest encryption and therefore the most fraud proof verification symbol possible.

Data compression is important for small portable data carriers employing two-dimension graphic symbols. The more verification data which one can incorporate in the verification symbols, the more effective the security and

verification of documents. There are three types of data compression, which are applied to four types of verification data.

Signature compression is used to compress scanned signatures. This compression is used primarily for the incorporation of signatures into two-dimensional verification symbols for personal cheques. It is used to compare the signature on a cheque with that incorporated within the verification symbol.

Facial compression is also used to compress digital facial images. These are used to verify ownership of private cheques and other personal documents.

This form of compression is necessary if one wishes to incorporate signatures within the restricted storage capacity of a two-dimensional symbol, as scanned signatures are digital raster images which consume large amounts of storage. Since this is a digital image compression it is a "lossy" compression (a compression which disposes of less relevant data).

Text data compression is used in all the verification symbols (two-dimensional symbols) of documents. There is normally a substantial amount of data required for the complete verification of documents and a high ratio "lossless" text compression (a compression which does not dispose of any data during the compression process) is needed. The compression allows for the entire verification record to be incorporated on a document.

Fingerprint biometric data acquisition and compression is required to be able to incorporate fingerprint biometrics into the document verification two-dimensional symbols. This compression is a "lossy" type of data compression.

The fingerprint biometrics are used in the verification symbols when absolute accountability is required for document verification. The fingerprint biometric scanner used can be a commercially available fingerprint matching product.

The above mentioned secure form of fingerprint verification as well as highly compressed fingerprint biometric data are the two main elements of security, absolute verification and definite accountability. This technology allows for verified and secure access to the system as well as ensuring accountability throughout the life cycle of a document. Since the compressed biometric data can travel with the document within a two-dimensional symbol, accountability data travels with the document and can be determined at any stage.

The encrypted symbol code which is printed on the document can be regarded as an extension of a traditional linear bar code, in that it is a printed symbol which facilitates machine reading thereof. A conventional bar code is only capable of representing enough data (typically 8 to 12 characters) to serve as a key to a more comprehensive database or record. The two dimensional graphic code used by the present invention, on the other hand, has sufficient capacity, especially using the compression methods described above, to hold an entire data record containing a substantial amount of data. In other words, the printed symbol is not merely a reference to a record stored elsewhere, but itself comprises a complete record.

The printed symbols also carry user definable levels of error correction. The error correction used allows for one hundred percent recoverability of the data contained in the symbol when the symbol suffers damage which is less than a predetermined maximum damage threshold. This makes the system relatively robust.

In document verification, use can be made of various two dimensional symbols commercially available (PDF417, Supercode and Aztec, for example) as well as proprietary two-dimensional codes or symbols. The choice of two-dimensional code depends on the suitability to the particular application and the intended scanning hardware.

For the purpose of mass printing at printing bureaux, a font based symbology was developed. This was necessary so that high speed printing bureaux do not require huge amounts of memory for large batches and so that production is not slowed down.

During the creation stage the relevant verification data and accountability data is compressed and encrypted and encoded into a two-dimensional bitmap image. This bitmap image or font set representing the symbol can be attached to any document and printed. The images are used in different manners depending on the type of document verification they are been used for.

In cheque verification a single two-dimensional symbol or code is printed on the cheque. The monetary amount, to whom the cheque is payable, the creation date, the expiry date and all other relevant data as well as authority and accountability data is incorporated into the two-dimensional symbol.

In other forms of document verification, the relevant data plus authority data is incorporated in a symbol as with the above mentioned cheque verification. In addition to this key portions of the document can be incorporated in compressed and encrypted two-dimensional symbols or, in the case when total privacy is required, the entire document can be incorporated in a set of two-dimensional symbols.

Once the two-dimensional code has been created it can be printed on the document using a conventional printer and the document is ready for distribution.

The document creation system comprises one or more document creation stations. Each document creation station has all the relevant software for access control and the software for data compression and encryption and the

generation of the two-dimensional verification symbol. The document creation station is connected to the online verification database server by a local area network (LAN) if the verification database server is on the same premises or by a wide area network (WAN) if the verification database server is at a remote site. Instead of a LAN or WAN, other communication systems such as a VPN, the Internet/WWW, spread spectrum radio, satellite link or a GSM network could be used, for example. There are two forms of creation stations:

A **stand-alone creation station**: On this type of station, all the functions of document creation are carried out on the workstation. The creation of the document, the creation of the compressed and encrypted two-dimensional code and the printing of the document are carried out at the station. The station is connected to a printer or a number of printers so that the documents can be printed.

A **document symbol server**: The server is part of the LAN or WAN. The documents are not generated on the server. Only the verification data is sent to this server. The server records the verification data as a record on the central verification database. It then creates the compressed and encrypted two-dimensional code (in bitmap image form) and dispatches this symbol to the system which created the document.

The document creation station preferably includes a test system including a two-dimensional scanner, which can be a hand held scanner or a flat bed document scanner. This scanner is used to test the printed two-dimensional symbols on documents created by the system.

As mentioned above, distribution of the documents created by the method of the invention is flexible, since each document is self-verifying due to the printing of tamper proof machine-readable data on the document itself. For example, in the case of a cheque which is mailed to a recipient thereof, a third

party who intercepts the cheque will not be able to read or alter the printed verification data on the cheque, so that even if the name of the payee or the amount of the cheque were to be altered, subsequent verification of the cheque will reveal the discrepancy.

Verification of the documents generated by the method of the invention is carried out in order to detect any fraudulent manipulation or tampering which has taken place, or even fraudulent creation of a document. Accountability for the document is also established and can be recorded where necessary. In some cases, typically in the case of cheque verification where payment takes place following the verification procedure, the payment details are entered against the verification data in the verification database, which prevents duplicate payments from being made.

Various levels of access control to the document verification stage of the method can be provided. The access control level depends on the level of security required, the type of document verification and the form of document verification. The lowest level of access control is merely a PIN code and is used in remote offline verification. In mass document verification systems, especially those which verify documents of monetary value, the highest level of access control is used. This latter form of access control is the same as that described above with regard to document creation. Here, the use of access cards which contain finger print biometric data ensures that absolute access control is established, as well as accountability. Since there are a few distinct forms of document verification, each form is described separately below.

Remote off-line verification is used in cases where on-line connectivity is not possible and where remote offline verification is necessary. The verification can be carried out on a portable hand held device, a laptop PC, or a conventional desk top PC. The system also makes use of remote two

dimensional scanners which are battery operated or powered by the portable host computer device.

Remote verification can also take place by means of hand held computers with built-in scanners since these are programmable. Access control and verification programs are stored and executed on these devices.

Remote off-line verification can be carried out manually, in which case a two-dimensional scanner is attached to the PC or portable computer. The two-dimensional symbol or each symbol is scanned. The symbol is decoded, decompressed and decrypted. The data derived from the two-dimensional symbol is then displayed. The operator can determine the authenticity of the document and also review the accountability and authority of the document. In some forms of document verification the contents can be manually verified against those of the document. This is the case in the remote cheque verification system.

Alternatively, the remote off-line system can use automated OCR/ICR technology. This form of verification has particular applications when remotely verifying documents of monetary value such as cheques. An A4 hand-held scanner is used for this process. The entire document is scanned. The writing on the document is converted to computer compatible text data by means of optical character recognition (OCR). The encrypted and compressed two-dimensional symbol is also decoded. The system compares the data derived from the two-dimensional bar code with that which was derived from the optical character recognition. Any discrepancies are highlighted and recorded.

On-line verification can utilise manual or high speed batch scanning. This first form of verification requires the operator to scan the document two-dimensional verification symbols with a handheld two-dimensional scanner or a hand held A4 document scanner. The online central verification database is

accessed. The record for the particular document, within the online verification database is compared to that the data record decoded out of the symbol. If there are any discrepancies, they are highlighted.

High speed batch verification is the most sophisticated system. It is used primarily for high speed automated verification of documents of monetary value. It is a main component of a typical cheque verification system of the invention and provides a highly secure and computer automated cheque verification center for banks. The main component of this system is a verification work station. This work station has the following software:

Access control and accountability software

This software restricts access to the system and also created an accountability log of the verifying operator.

Image based two-dimensional symbol decoding software

Since the cheques are scanned in batches by a scanner or a number of scanners (document flatbed scanners with automatic document feeders), the two-dimensional symbol decoding software is image based. The symbol is detected and decoded.

Decompression and decryption software

This software decompresses the decoded symbol data and then decrypts the data.

Interface software to high speed document scanners

This is image acquisition software which acquires the images from the high speed document scanners.

Image processing software

This is highly specialized image processing software which cleans up and enhances the document image so that the two-dimensional bar code can be easily decoded. The document cleanup also aids the OCR software.

OCR software

The purpose of the optical recognition software is a first phase verification of the printed data on the cheque with the data acquired from the two-dimensional symbol. The OCR software used in the prototype system is based on backward propagation neural network technology as well as sophisticated image extraction techniques. The neural network is trainable and can be trained to identify various fonts as well as partially visible letters and numbers.

The automated high speed verification process is conducted as follows. The documents are loaded into the automatic document feeder of the scanner. The software interface to the scanner triggers the document feeder so that the documents are automatically fed into the scanner and then scanned. The document images are then processed by the image processing software. The printed characters are extracted and identified by the optical character recognition. The two-dimensional symbol is then extracted and the data is decoded, decompressed and decrypted. The data acquired from the two-dimensional symbol is compared with the results of the optical character recognition. If there are any discrepancies in the comparison, they are recorded in the central verification database record for the particular document.

The data extracted from the two-dimensional verification symbol is then compared to the authentication record in the central verification database record. If there are discrepancies the document is marked as fraudulent. The system also verifies that the document has not been previously paid in the case of verification of cheques and other documents of monetary value. In the case of documents of monetary value the system will approve payment of the document or cheque if it is satisfied that the document is fraud-free and has

not already been paid on. All statuses are recorded in the central verification database. The entire process is automated and requires (and will not allow) any human intervention.

The central verification database is central to the process described above. All actions relating to a document are recorded in this database. The contents of the database are encrypted and a secure hardware device controls the encryption.

The encryption encoding is set by a person who has due authority to carry out this task. Each time a document is created the verification data of the document is recorded in the verification database. A duplication of this record is used to create the printable two-dimensional verification symbol which travels with the document. When a document is verified the data acquired from the verification symbol is compared with the original database record. All results of the document verification process are recorded in the verification database in the appropriate document record.

In order to permit enquiries to be made via the enquiry stations 18, the central verification database can be accessed for this purpose. Examples of enquiries which can be made include the following:

- On whose authority was the document created?
- Who created the document?
- On what date was the document created?
- For cheques:

  The expiry date.
  The amount.
  The payee.
  The bank details and cheque number.

The signatories.

Was the cheque paid and if so, when?

Who verified it?

- Was the document identified as fraudulent and if so, what was the nature of the fraud?

The inquiry system can also supply statistical reports, such as information on how many documents of a certain value were detected as being fraudulent.

An image of each document, which is acquired from the document image scanner during the verification process, is stored and indexed in an archive controlled database. Preferably, the images are stored on optical storage media. These images can be used in the case of a dispute, and the encrypted symbols on the images can also be used recreate the database in a disaster recovery situation.

CLAIMS:

1. A method of generating a document comprising the steps of:

permitting access to a document creation system by an authorised user;

recording user data identifying the user;

generating document data defining a document;

generating verification data from the user data and the document data;

printing the document utilising the document data and the verification data, so that the document includes a machine readable portion usable to verify the authenticity thereof.

2. A method according to claim 1 including generating a user identification record and storing the record for comparison with the user data when a user attempts to access the document creation system.

3. A method according to claim 2 wherein the user data and the user identification comprise data from a fingerprint scanner or another biometric device.

4. A method according to any one of claims 1 to 3 wherein the user data is derived from data stored on a portable data carrier, the user data being generated when a physical characteristic of the user matches data stored on the portable data carrier.

5. A method according to claim 4 wherein the portable data carrier is a smart card.

6. A method according to claim 4 or claim 5 wherein the physical characteristics of the user is a fingerprint or other biometric data.

7. A method according to any one of claims 1 to 6 wherein the authentication data is stored in a document verification database.

8. A method according to claim 7 wherein the verification data takes the form of a bar code, symbol or other machine readable indicium.

9. A method according to claim 7 or claim 8 wherein the verification data is a printed symbol or code readable optically, and contains data which corresponds at least partially to the user data and the related document data contained in the authentication data which is stored in the document verification database.

10. A method according to claim 9 wherein the verification data comprises one or more of the following: details of an operator generating the document, date/time stamps, a unique document and/or institution code, partial or relevant details from the document, digital signature of the operator and/or competent authority, a digital certificate, a facial image of a relevant person; a digital image of a hand written signature, a fingerprint or other biometric data, or textual information.

11. A method according to claim 9 or claim 10 wherein the verification data is generated in an encrypted form.

12. A method of verifying the authenticity of a document generated by the method of any one of claims 1 to 11, the method including the steps of:

reading verification data from the document;

retrieving authentication data corresponding to the verification data and comparing the verification data with the authentication data; and

indicating that the document is authentic if the compared data matches.

13. A method according to claim 12 wherein the verification data is encrypted, the method including the step of decrypting the verification data read from the document.

14. A method according to claim 12 or claim 13 wherein the authentication data is retrieved from a central database in an on-line process.

15. A method according to claim 12 or claim 13 wherein the authentication data is data derived from the document itself or from the bearer thereof.

16. A system for generating documents comprising:

a document creation station operable by a user to input document data and to generate printed documents based on the document data;

access control means arranged to generate user data corresponding to an authorised user;

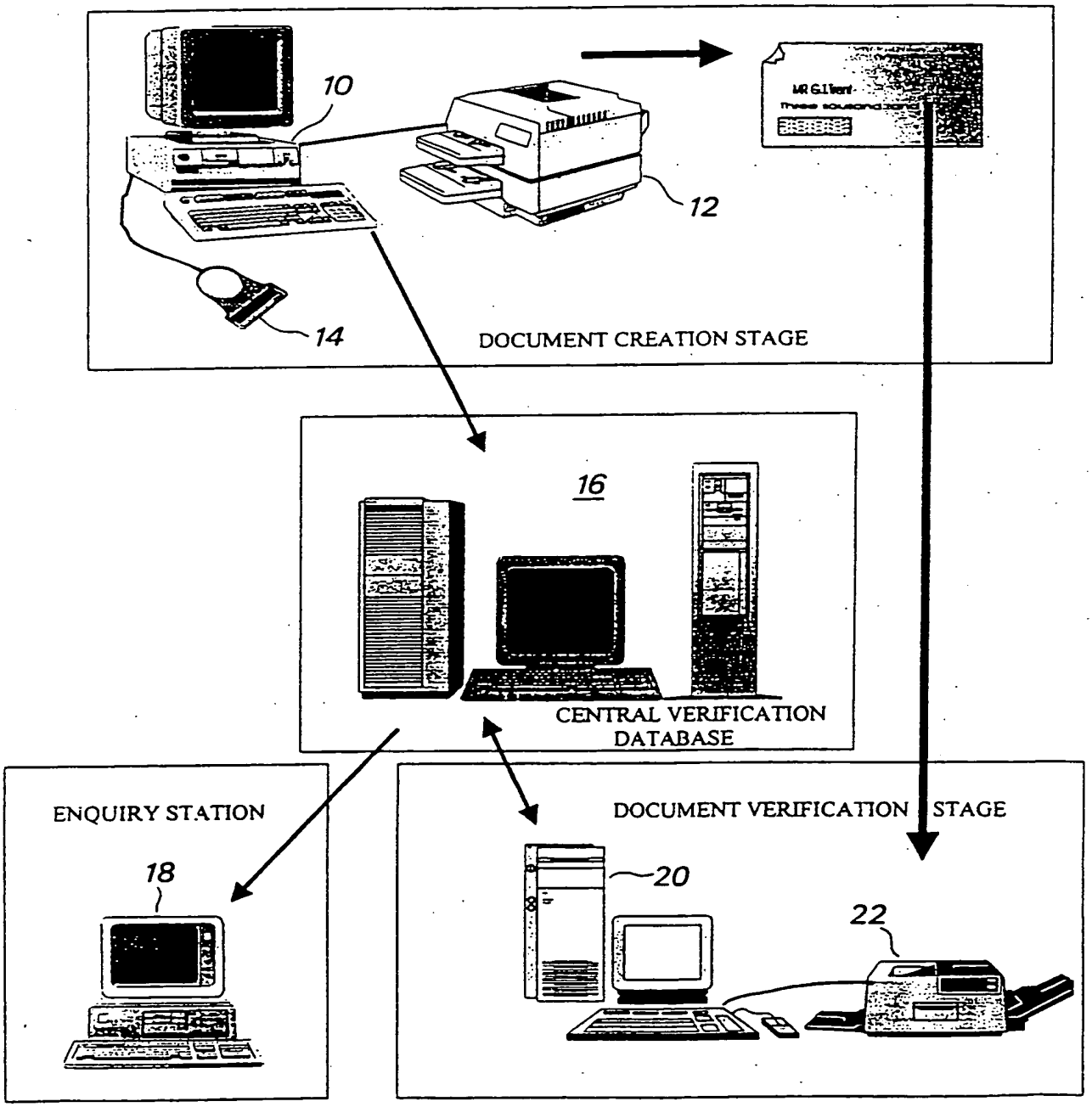
processor means for generating verification data derived from the document data and the user data, the verification data being applied to the printed document; and

a database for storing an authentication record corresponding to the verification data, for use in authentication of the document.

17. A system according to claim 16 including at least one document reading device for reading the verification data on a document, and processor means for comparing the verification data read from the document with authentication data.

18. A system according to claim 17 including communication means for transferring authentication data from the database, for comparison with the verification data read from the document.

Fig 1


10
12
14
DOCUMENT CREATION STAGE
16
CENTRAL VERIFICATION DATABASE
ENQUIRY STATION
18
DOCUMENT VERIFICATION STAGE
20
22

This Page Blank (us

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB 00/00908

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07D7/00 G07F7/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07D G07F G03G G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 547 837 A (XEROX CORP) 23 June 1993 (1993-06-23) abstract column 1, line 14 - line 24 column 2, line 18 - line 30 column 5, line 23 - line 33	1-6,12, 13,15
Y	column 8, line 35 -column 10, line 54	7,16
Y	WO 95 23388 A (BLANCHESTER TOM ;NON STOP INFO AB (SE)) 31 August 1995 (1995-08-31) abstract	7,16
A	US 5 270 773 A (SKLUT ROBERT L ET AL) 14 December 1993 (1993-12-14) abstract	1

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 November 2000	08/12/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Lindholm, A-M

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 022 080 A (DURST ROBERT T ET AL) 4 June 1991 (1991-06-04) column 2, line 40 -column 3, line 40 column 5, line 1 - line 12	1
A	PATENT ABSTRACTS OF JAPAN vol. 1999, no. 04, 30 April 1999 (1999-04-30) & JP 11 003456 A (NIPPON TELEGR &TELEPH CORP <NTT>), 6 January 1999 (1999-01-06) abstract	7,16

INTERNATIONAL SEARCH REPORT

Information on patent family members

In[illegible]ional Application No
PCT/IB 00/00908

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0547837 A	23-06-1993	US 5157726 A	20-10-1992
		JP 6176036 A	24-06-1994
WO 9523388 A	31-08-1995	SE 502658 C	04-12-1995
		AU 1905395 A	11-09-1995
		SE 9400686 A	29-08-1995
		US 6141438 A	31-10-2000
US 5270773 A	14-12-1993	NONE	
US 5022080 A	04-06-1991	CA 2043533 A,C	01-12-1992
		JP 6014018 A	21-01-1994
		EP 0516898 A	09-12-1992
JP 11003456 A	06-01-1999	JP 2938832 B	25-08-1999